EXHIBIT 4:

Application for Search Warrant
21-cr-00155-DJH-RSE (W.D. Ky. Feb 8, 2020)

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, John C. Koski, Jr., a Special Agent with the United States Department of Homeland Security (DHS), Immigration and Customs and Enforcement (ICE), Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1) I am a Special Agent (SA) employed by the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) and I have been so employed since May 2005. I am currently assigned to HSI Louisville, Kentucky.

2) As part of my official duties as an HSI Special Agent, I investigate criminal violations relating to the sexual exploitation of children and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, et. seq. I have received training in the area of child pornography and child exploitation investigations and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256(8)(A)), in all forms of media including computer media during law enforcement training and experiences. I have also received training and instruction in the field of investigating child pornography.

3) As a result of my training and experience, I am familiar with methods employed by individuals engaged in various illegal activities, including interstate transportation of child pornography. I am also aware from my training and experience that persons engaged in interstate transportation of child pornography typically use false identities and other techniques

to disguise themselves and their enterprise. I am further aware, as a result of my training and experience that child pornography is not generally available in retail establishments, even from those which offer other explicit sexual material. Persons who wish to obtain child pornography do so by ordering and/or obtaining it by discreet contact with other individuals and underground businesses that have child pornography collections.

4) This affidavit is submitted in support of an application for a search warrant for the location specifically described in **Attachment A**, including the entire property and vehicles located at 2134 Woodbourne Ave, Louisville, KY 40205 (the "SUBJECT PREMISES"), the content of electronic storage devices located therein, and any person located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A, relating to material involving the sexual exploitation of minors, which items are more specifically described in **Attachment B**.

5) The statements contained in this affidavit are based in part on information provided by United States federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; independent investigation and analysis by law enforcement officials/ agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent with HSI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of

violations of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (accessing with the intent to view child pornography) are presently located at the SUBJECT PREMISES.

DEFINITIONS

6) The following definitions apply to this Affidavit and Attachment B:

a) "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.

b) "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c) "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

d) "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e) "Child pornography," as that term is defined in 18 U.S.C. § 2256(8)(A).

f) "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

g) "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

h) "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

i) "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j) The "Domain Name System" or "DNS" is system that translates readable Internet domain names such as www.justice.gov into the numerical IP addresses of the computer server that hosts the website.

k) "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

l) A "hidden service," also known as an "onion service," is website or other web service that is accessible only to users operating within the Tor anonymity network.

m) "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

n) The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices

on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o) "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

p) An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

q) "Minor," as that term is defined in 18 U.S.C. § 2256(1).

r) "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

s) "Remote computing service," as that term is defined in 18 U.S.C. § 2711(2).

t) "Sexually explicit conduct," as that term is defined in 18 U.S.C. § 2256(2).

u) A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

v) The "Tor network" is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit."

w) "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting

one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

x) "Visual depiction," as that term is defined in 18 U.S.C. § 2256(5).

y) A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

7) A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography *via* a hidden service website that operated on the Tor anonymity network. The website is described below and referred to herein as the "TARGET WEBSITE."[1] There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE, as further described herein.

The Tor Network

8) The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content

[1] The name of the TARGET WEBSITE is known to law enforcement. Investigation into the users of the website remains ongoing and disclosure of the name of the website would potentially alert active website users to the investigation, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

9) The website further described below operated on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective.

10) To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.[2] The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network.

11) As with other Internet communications, a Tor user's communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be

[2] Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

12) Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses such an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

13) The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

14) The Tor Network also makes it possible for users to operate or access websites that are accessible only to users operating within the Tor network. Such websites are called "hidden services" or "onion services." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

15) Unlike standard Internet websites, a Tor-based web address is comprised of a series of either 16 or 56 algorithm-generated characters, for example "asdlk8fs9dflku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

Description of TARGET WEBSITE

16) The TARGET WEBSITE was an active online chat site whose primary purpose was to share and distribute child pornography. The advertisement and distribution of child pornography and child erotica were regular occurrences on this site. On the front page of the site, it stated that the site was intended for users to "post links with good photos and videos" depicting "[o]nly GIRLS 5 to 13 years [old]." The TARGET WEBSITE started operating in approximately 2018. The site allowed users to engage in online chat with other users, either within chat rooms that were openly accessible to any user of the site, within rooms only accessible to particular users, or in one-to-one chats between two users. Child pornography

images and videos were trafficked through this chat site via the posting of web links within chat messages. Links allowed a user to navigate to another website, such as a file-hosting website, where images and/or videos were stored in order to download these image and videos. The TARGET WEBSITE provided its users with information about particular file hosting websites where users could upload digital files so that the files could then be shared, via links, with other users on the TARGET WEBSITE.

17) Entry to the site is obtained through free registration, as described below. On the registration page, it reads, among other things, "No hurtcore, No gore, No zoo, No death, No toddlers." In my training and experience, "zoo" refers to pornography depicting bestiality, and "hurtcore" is a genre of child pornography that depicts violence, gore, torture, humiliation, or children in pain and distress. In addition, the registration page of the TARGET WEBSITE expressly contemplated the sharing of videos between members. Language on that page reads "Post links with good photos and videos (preview is required!)."

18) In order to pass through the registration page and gain access to the actual content of the TARGET WEBSITE, a prospective user must create a "Nickname" and a password which must be entered along with a Captcha. A "Captcha" is a randomly generated series of characters designed to ensure that users of a website are human beings and not bots or other automated processes. Users are not required to enter any personally identifiable information, such as true names, emails or phone numbers. The users may also pick a color for their posts or one was randomly generated and clicked "enter chat."

19) Upon initially registering a user account on the TARGET WEBSITE, a user is assigned the status of "Guest." After registering a user account on the TARGET WEBSITE, a

user must log in to that user account with the appropriate user-generated password in order to communicate via that user account on the TARGET WEBSITE. TARGET WEBSITE users may register, log into and access the TARGET WEBSITE through that user account using any computer or electronic device that is configured to use Tor routing/software.

20) As is common on these types of sites, the TARGET WEBSITE was administered and moderated by select TARGET WEBSITE users referred to as "Members" on this site. These users are promoted at the discretion of the site leadership. Promotions appeared to be made based on an individual's active participation on the site. Once promoted to a Member position, those users enforced the rules and assisted in the management of the site. This included controlling user membership using the "ban" and "kick" functions (which can limit or eliminate a user's participation or account), promoting within the ranks of users, and moderating the public chatroom for content and user behavior.

21) TARGET WEBSITE Members periodically re-posted standard messages to the public chatroom of the TARGET WEBSITE iterating rules and procedures of the TARGET WEBSITE. For example, on or about May 28, 2019, a Member on the TARGET WEBSITE posted "CHAT RULES" in the public chatroom. This post contained statements in both Russian and English which included but was not limited to, "Follow the requests of the Members", "No hurtcore, No gore, No zoo, No death, No toddler", "Only GIRLS 5 to 13 years. Any language allowed", and "For RG (registered guests) the photo archive is available (the "links" button)."

22) On or about May 28, 2019, a Member posted "SECURITY INFORMATION" in the public chatroom. This post contained statements in both Russian and English which included but was not limited to the following:

- Set the Security Slider to HIGH Security Level
- Do Not Download if you are not using Encryption or Tails OS
- Read these manuals: → Tails Guide & Tor Security Guide ←

Do Not Share any Identifying Information & NEVER Trust Anybody!

Windows & OS X/MacOS are not safe for On topic

Save files only to Ecrypted Storage

Windows Leaves traces you cannot clean without a Full disk wipe

Linux offers Full Disk Encryption, Tails is Amnesic

use VeraCrypt to create Hidden Encrypted Containers

Open files when Offline to lower risk of malicious file causing trouble

LEA & Antis are known to pose as parents and kids to trick you into revealing information to them, suspect everyone is LEA.

LEA could be running this or any site at any time

Always be conscious your messages may not be private

Be Careful Paying for Anything, Bitcoin is not Anonymous by default!

23) When a user posts in the open chat, other users can see the name of the poster, what was posted and what time it was posted. Images posted to the site can be categorized or "tagged" by users based upon the image theme or characteristics. These tags aid users in searching for specific types of content.

24) There was also an advertisement in the middle of the TARGET WEBSITE chat screen stating, "VISIT OUR SITES" and it features four links to other Tor sites. Each site has a short description along with a link to the Tor web address for the site. The descriptions state:

"Forum for boy-and girlovers" with a link to another website; "Chat for boylovers" – with a link to another website; "Girls pedo portal", and "only Ru". Based on my training and experience, I am aware that the reference to "only Ru" means that site is only for Russian speakers. Further, based on my training and experience, it is apparent that these websites are associated with each other.

25) The TARGET WEBSITE provides users with links to image hosts where users can upload their digital images. For instance, on November 2, 2018, a TARGET WEBSITE user posted a hyperlink of a .jpeg file named https://MATRIX_171313_cae_178991.jpg that linked to an image of a prepubescent girl having her underwear pulled down and a male penis resting on her inner thigh near her exposed vagina. FBI Special Agents have accessed and downloaded child pornography files via links that were posted on TARGET WEBSITE, in an undercover capacity, from computers located in the District of Maryland.

26) Hidden service websites on the Tor Network are not "indexed" by search engines – such as Google – to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult, if not impossible, to perform a Google-type search of the Tor Network looking for child exploitation and pornography related websites that operate on that network. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) accordingly keep and maintain directory sites that advertise the web addresses for such sites. Users utilize those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to the exploitation of children. The Tor network web address for TARGET WEBSITE was listed on one or more such directory sites advertising hidden services dedicated to the sexual

exploitation of children. Postings to the TARGET WEBSITE that were publicly available to any registered user at the time of posting were captured and archived for law enforcement review. Over 947,000 messages were posted on the TARGET WEBSITE between March 2018 and May 2019. Many of those postings included links to images which were also captured and archived.

Evidence Related to Identification of Target that Accessed TARGET WEBSITE

27) I am aware that United States, as well as foreign, law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as the websites described herein. Those websites are globally accessible. The websites and their users may therefore be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, it is common practice for that law enforcement agency to share information with a law enforcement agency in the country where the website is located or the offender appears to reside, in accordance with each country's laws.

28) HSI Special Agents received information from a foreign law enforcement agency (referenced herein as "FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that FLA determined that on April 11, 2019, IP address 104.49.245.246 "was used to access online child sexual abuse and exploitation material" *via* a website that the FLA named and described as the TARGET WEBSITE. The FLA was able to identify the IP address 104.49.245.246 utilizing FLA established legal undercover methodologies and techniques.

29) Affiant received and reviewed several files depicting child sexual abuse that were available on the TARGET WEBSITE when the user connected to IP address 104.49.245.246 accessed the site. Descriptions for a sampling of the files[3] are set out as follows:

a) Image – File Name 1556381394.jpg – The image depicts a naked adult male inserting the tip of his penis into the vagina of a little girl (approximately age six to nine based on body size in proportion to the man, lack of breast development, and no pubic hair.) The little girl is completely nude and lying on her back on a bed. Her legs are spread apart with knees bent over the man's legs. Her arms are crossed. The photo does not show the face of the man or little girl.

b) Image – File Name Felixxx_185145_Cho_.jpg – The image depicts a little girl (approximately five to eight years old based on body size, lack of breast development, and no pubic hair). She is standing naked in a bathtub. The girl is standing on her left leg while holding her right leg in the air with her right arm. Her legs are spread apart, revealing her exposed genitals.

c) Image – File Name twlba5j7oo5g4kj5.onion (1).jpeg – The image depicts a little girl (approximately five to eight years old based on body size in proportion to the man and lack of breast development). She is naked and lying on her back. A naked, adult man is standing over the little girl. She is holding his erect penis with both hands. The man's face is not shown. But, the little girl's face is visible.

30) FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of United States law enforcement sharing criminal investigative information with FLA and FLA sharing criminal investigative information with United States law enforcement, across disciplines and including the investigation of crimes against children. FLA advised United States law enforcement that it obtained that information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws. FLA further advised United States law enforcement that FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain

[3] Still images of the files referenced in numbered paragraph 29(a) – (c) have been shown to the reviewing Magistrate Judge and will be maintained in a secure manner by Affiant.

that IP address information. United States law enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

31) I am aware through my training and experience and consultation with other United States law enforcement agents that tips provided by FLA regarding IP addresses that FLA advised were associated with access to Tor network child exploitation-related web and chat sites have: (1) led to the identification and arrest of a United States-based child pornography producer and hands-on offender, and the identification and rescue of multiple United States children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that United States law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

32) As described herein, the TARGET WEBSITE could not generally be accessed through the traditional internet. Only a user who had installed the appropriate Tor software on the user's computer could access the "TARGET WEBSITE." Even after connecting to the Tor network, however, a user would have to find the 16-or-56-character web address of the TARGET WEBSITE in order to access it. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitation related

content. Those directory sites also operate via the Tor network. Users utilize those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or "hurtcore"). They also contain clickable hyperlinks to access those sites. As with other hidden service websites, a user must find the 16-or-56 character web address for a directory website in order to access it. While it operated, the web address for the website described herein was listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children.

33) I am also aware through consultation with FBI agents that the review of detailed user data related to one Tor network based child pornography website found that it was exceedingly rare for a registered website user to access that website and never return. FBI review of user data from that website found that less than two hundredths of one percent of user accounts registered an account on the website, accessed a message thread on the website, and then never returned to the website and logged in to the same account.

34) Accordingly, based on my training and experience and the information articulated herein, because accessing the TARGET WEBSITE required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor – it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.

35) Accordingly, I submit that there is probable cause to believe that, for all of the reasons described herein, any user who accessed the TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so, in violation of 18 U.S.C. § 2252A(a)(5)(B).

Identification of SUBJECT PREMISES

36) According to publicly available information, IP address 104.49.245.246, which was used to access TARGET WEBSITE on April 11, 2019, was registered to AT&T.

37) On November 22, 2019, a subpoena/summons was issued to AT&T in regard to the pertinent IP address. A review of the results obtained on November 23, 2019, identified the following account holder and address, which is the address of the SUBJECT PREMISES:

- Subscriber Name: Joshua White
- Service Address: 2134 Woodbourne Ave, Louisville, KY 40205
- Start of Service: May 8, 2017
- End of Service: May 30, 2019
- Account IP: 104.49.245.246

38) A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for Joshua White on April 8, 2020. These public records indicated that White's current address is 2134 Woodbourne Ave, Louisville, KY 40205.

39) A check with the Kentucky Department of Motor Vehicles on or about May 13, 2020, revealed that an individual named Joshua White resides at the SUBJECT PREMISES.

40) A check of open source information from the Internet regarding Joshua Whtite revealed that he is a Contractor/Consultant the provides electronic circuit design and review in Louisville, Kentucky. The check also revealed that Joshua White is married.

41) On November 9, 2020, HSI Special Agent Michael Huffines conducted surveillance of the residence located at 2134 Woodbourne Ave., Louisville, Kentucky. During this time, SA Huffines observed a tan colored Chevy pickup truck with a Kentucky license plated of 071YTV. A search conducted of the Kentucky Department of Motor Vehicles showed this vehicle as a 1998 Chevy Truck, a VIN number of [redacted], a registered owner of Joshua White with a social security number of [redacted], a registered address of 2134 Woodbourne Ave, Louisville, Kentucky (SUBJECT PREMISES), and a vehicle registration date of September 8, 2020.

42) On January 13, 2021, a search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for the address of 2134 Woodbourne Ave, Louisville, Kentucky. These public records indicated that as of September 2020, Joshua White continued to reside at the above address.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

43) I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a) Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b) Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c) A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d) The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e) The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f) Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g) A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h) As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital

information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

44) Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via a website:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[4]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g. online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

45) Based on all of the information contained herein, I believe that an internet user residing at the SUBJECT PREMISES likely displays characteristics common to individuals who access online child sexual abuse and exploitation material via a website. In particular, the target of investigation obtained and used Tor network software, found the web address for TARGET WEBSITE, and accessed online child sexual abuse and exploitation material via the TARGET WEBSITE.

[4] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

46) As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Fed. R. Crim. P. 41(e)(2)(B).

47) I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

48) As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such

information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data

that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

49) Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

50) Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

51) Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

52) Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

53) I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

/s/ John C. Koski, Jr.
John C. Koski Jr.
Special Agent

Sworn to/attested to by the affiant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone and email, reliable electronic means, this 8th day of February, 2021.

REGINA S. EDWARDS
United States Magistrate Judge

MAB:JEL